Third Party Risk Management **Checklist**

venminder

Vendor Management Program Documentation

- [ ] Create or update a vendor management policy
- [ ] Create or update a vendor management program
- [ ] Create or update vendor management procedures

Foundational Documents/Baseline Due Diligence

These should be used from the vetting process through ongoing oversight and monitoring.

- [ ] Mutual Non-Disclosure Agreement (MNDA) or Confidentiality Agreement
- [ ] Basic Information (full legal name, address, all physical locations, website URL)
- [ ] Ownership structure and affiliated companies
- [ ] Tax ID
- [ ] State of Incorporation
- [ ] Articles of Incorporation
- [ ] Secretary of State Check
- [ ] Business license
- [ ] Certificate of Good Standing
- [ ] Credit report
- [ ] OFAC/PEP checks
- [ ] Any "doing business as" or "also/previously known as" (d/b/a, aka, pka)
- [ ] Dun & Bradstreet (D&B) report
- [ ] Vendor complaints research findings
- [ ] Vendor negative news search findings
- [ ] List of subcontractors / fourth parties
- [ ] Picture or Google map view of facility (if required)
- [ ] Conduct check of CFPB Complaint Database and/or Better Business Bureau rating

**Some of the other documents listed in this checklist may be a foundational document request, too (e.g., financials, SOC report, business continuity plan).*

Due Diligence Often Required (in addition to foundational/baseline requirements)

These should be used from the vetting process through ongoing oversight and monitoring.

FINANCIALS

- [ ] Annual report (if publicly traded)
- [ ] 3 years audited financials
- [ ] Accountant's statement

EXAMINATIONS AND REPORTS

- [ ] Reports of internal and external audits
- [ ] Regulatory regional office record of audit reports (FI's must request directly)
- [ ] Information security penetration testing
- [ ] Vulnerability testing
- [ ] Business continuity plan and testing
- [ ] Disaster recovery plan and testing
- [ ] SSAE 18, SOC 1, 2 or 3 and bridge letter, if needed

LICENSES OR PROFESSIONAL CERTIFICATIONS

- [ ] Any required licenses (e.g., state money transmitter license)
- [ ] PCI certification/QSA letter
- [ ] ISO certification
- [ ] Proof of admission to the bar for state practices

INSURANCE

- [ ] General liability
- [ ] Cyber insurance
- [ ] Employee malfeasance
- [ ] Specific insurance standards required by business lines

EDUCATION

- [ ] Biographies of key managers and ownership (if needed)
- [ ] Compliance education schedule
- [ ] Change management education schedule

DIAGRAMS

- [ ] Network diagram
- [ ] Data flow diagram, including any third party/fourth party
- [ ] Organization chart of affiliated companies and holding company
- [ ] Organization chart of staff
- [ ] IVR/call routing flows

SLAs

- [ ] Record of outages and SLA violations (usually a contractual obligation)

SITE VISITS

- [ ] Potential on-site visit, if needed

POLICIES AND PROCEDURES

- [ ] Compliance policies
- [ ] AML detection policies
- [ ] Scripting policy (call centers)
- [ ] Change management policy
- [ ] Data protection/information security policy
- [ ] Business continuity plan (including pandemic policy)
- [ ] Record retention/data destruction policy
- [ ] Hiring policy
- [ ] Drug testing policy
- [ ] Background check policy
- [ ] Media policy
- [ ] Vendor management policy
- [ ] Complaint management policy/complaint escalation procedure
- [ ] Logical account management policy
- [ ] Plans, protocols and results

**The above is a list of the due diligence requirements we often see. However, due diligence requirements are based on the organization's policy and the vendor relationship's criticality and risk level to the organization.*

Risk Assessments

- [ ] Determine business impact risk rating (critical or non-critical)
- [ ] Determine regulatory risk rating (typically low, medium or high risk based on categories of risk such as strategic, reputation, operational, etc.)

Contracts

Provisions to Include:

- [ ] Scope of service
- [ ] Rights/responsibilities of the parties
- [ ] Pricing methods
- [ ] Term/renewals/termination
- [ ] Performance standards
- [ ] Liability
- [ ] Indemnification
- [ ] Proprietary information
- [ ] Security and confidentiality
- [ ] Internal controls
- [ ] Reports
- [ ] Business Continuity
- [ ] Subcontracting
- [ ] Compliance with applicable laws and regulatory expectations
- [ ] Right to Audit

Contract Management

- [ ] Internal planning (know who is involved in the process)
- [ ] Negotiation/Creating/Drafting (know who is responsible)
- [ ] Approving/Executing (know who is authorized)
- [ ] Storing (central repository with tracking of significant dates)
- [ ] Managing (e.g., service delivery, performance, ongoing relationship)

Reporting

It's encouraged to provide reports on a regular, recurring basis to senior management, the board and your compliance and audit committees. A typical report contains the following with a page dedicated to each topic.

- [ ] Cover page with total inventory of actively managed third party vendors
- [ ] Overall inventory of third party vendors
- [ ] Overall status of assessing risk (e.g., perhaps a pie chart showing how many critical and non-critical or high, medium and low-risk third party vendors)
- [ ] Due diligence (e.g., how many documents, upcoming due diligence and any overdue or missing items)
- [ ] Ongoing monitoring activities (e.g., what your team is doing to meet this critical expectation)
- [ ] Contracts (e.g., upcoming renewals or terminations, any notable problems with critical or high-risk third party vendors)
- [ ] Any major changes with high-risk and/or critical third party vendors
- [ ] A calendar showing upcoming updates to various committees, helping to demonstrate management is adequately informed in an ongoing manner

Audit

How To – From Start to End

- [ ] Notify senior management and the board
- [ ] Review the audit notification
- [ ] Prepare talking points
- [ ] Plan (e.g., opening meeting, periodic updates, closing)
- [ ] Determine where the auditors will work
- [ ] Determine who the auditors may ask questions
- [ ] Establish a spokesperson
- [ ] Create or update the vendor management policy, program and procedures
- [ ] Review your vendor list (be prepared to discuss the different vendor types)
- [ ] Review the document request lists
- [ ] Fully understand the scope of vendor monitoring practices
- [ ] Review your prior examination report for unaddressed items
- [ ] Address any prior examination items that have been missed
- [ ] Compare the prior examination to the new notice for changes in scope
- [ ] Communicate with your team regarding expectations
- [ ] Clarify any potential concerns or why you've done something a particular way, if needed
- [ ] Reciprocate auditor feedback
- [ ] Take notes
- [ ] Ensure your work product matches what is outlined in your program
- [ ] Keep record of what you've provided

Download free work product samples
and see how Venminder can help reduce your vendor management workload.

SAVE CHECKLIST **PRINT** CHECKLIST

Copyright © 2019 by Venminder, Inc.